INEEL NATIONAL SECURITY

Preventing that Attack

RapidOps is a vulnerability assessment tool, linking time and probability modeling in a graphical, intuitive, easy to use, and field-deployable environment.

Idaho National Engineering and Environmental Laboratory
INEEL
Home of Science and Engineering Solutions

RapidOps

Assessing vulnerabilities from beginning to end

What is the probability that we can effectively prevent a terrorist attack against a key asset? If an intentional or natural disruption does occur, how quickly can we respond?

Key to thwarting possible terrorist attacks against our infrastructure - energy, banking, transportation, government or telecommunications - is improving our ability to understand and model threat-related attack sequences in duration (time) and probability (success), as well as associated defensive elements and response postures. RapidOps readily permits such analyses via an intuitive interface and strong graphics base.

RapidOps is an operational vulnerability assessment tool, which links time and probability modeling in a graphical, intuitive, easy-to-use, and field-deployable computer-assisted work environment. RapidOps can calculate and display the likelihood of success for various defenses (e.g., using various sensor types or locations, or using special response teams).

Various vulnerability assessment methods, tools, and systems have been developed for diverse uses and users. Unfortunately, although extremely powerful, many such developed systems are frequently not intuitive and,

Continued on back

Continued from front

therefore, restrict use to a select group of experts. In other instances, high-powered computer systems and related technical experts are required to run complex vulnerability simulation models.

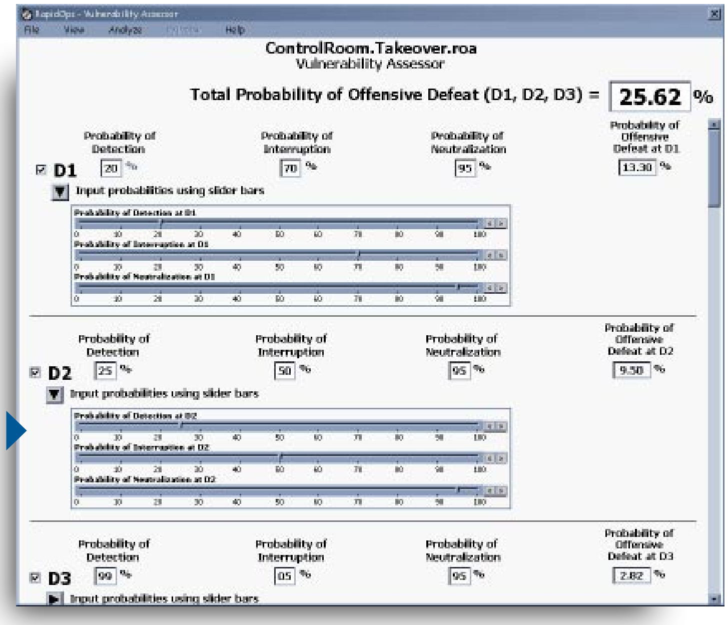
The vulnerability assessment approach implemented in RapidOps is similar to that used in the Department of Energy and other agencies concerned with the protection of physical assets. However, the goal of RapidOps is to allow users in diverse operational settings to create - via a PC or computer notebook - various time-critical, attack scenarios and assess their potential effectiveness, especially against fixed and variably defended targets.

By conducting multiple "what if..." scenarios, those users can examine the potential efficacy of in-place or proposed defensive postures and associated security systems. Such insights enable better understanding, analysis, and evaluation of the potential effectiveness and associated risks of such scenarios. The unique advancement of RapidOps is the simultaneous linkage of time and probability modeling in a graphic, intuitive, and easy-to-use, computer-assisted environment.

The RapidOps vulnerability assessment tool allows individuals with diverse backgrounds and skills, working independently or collaboratively, to investigate security and vulnerability issues related to physical asset protection. Applications for terrorist attack modeling and defensive response analysis can be completed with RapidOps.

RapidOps Key Features:

- PC-based
- Field-deployable
- Stand alone application
- Embedded support tools and look up databases
- Vulnerability assessment algorithms


RapidOps - Vulnerability Assessor
File
View
Analyze
Help
Probability of Detection at D1
0 10 20 30 40 50 60 70 80 90 100
Probability of Interruption at D1
0 10 20 30 40 50 60 70 80 90 100
Probability of Neutralization at D1
0 10 20 30 40 50 60 70 80 90 100
Probability of Detection at D2
0 10 20 30 40 50 60 70 80 90 100
Probability of Interruption at D2
0 10 20 30 40 50 60 70 80 90 100
Probability of Neutralization at D2
0 10 20 30 40 50 60 70 80 90 100

ControlRoom.Takeover.roa
Vulnerability Assessor

Total Probability of Offensive Defeat (D1, D2, D3) = 25.62 %

	Probability of Detection	Probability of Interruption	Probability of Neutralization	Probability of Offensive Defeat at D1
☑ D1	20 %	70 %	95 %	13.30 %

▼ Input probabilities using slider bars

	Probability of Detection	Probability of Interruption	Probability of Neutralization	Probability of Offensive Defeat at D2
☑ D2	25 %	50 %	95 %	9.50 %

▼ Input probabilities using slider bars

	Probability of Detection	Probability of Interruption	Probability of Neutralization	Probability of Offensive Defeat at D3
☑ D3	99 %	05 %	95 %	2.82 %

▶ Input probabilities using slider bars

RapidOps allows users to create multiple "what...if" scenarios to examine the effectiveness of existing or potential defensive postures of security systems.

- Graphical representations
- Quick results
- Minimal learning time
- User-friendly

RapidOps Methodology

- Develop attack scenarios with activity and operation planner and embedded support tools.
- Develop corresponding response scenarios.
- Automatically create event time lines and identify interruption points.
- Determine overall probability of success (of attack) using detection, interruption, and neutralization with vulnerability assessor at identified points.
- Assess outcomes and view summary charts.
- Make changes (e.g., add delays or change detection points based on additions of sensors or changes in defense response).
- Assess effects of changes.

Points of Contact:

Jerry Harbour
208-526-4301
harbgl@inel.gov

Ken Watts
208-526-9628
kdw@inel.gov